Remarks

The present amendment responds to the Official Action dated September 7, 2004. The Official Action rejected claim 7 under 35 U.S.C. §112, second paragraph due to insufficient antecedent basis. Claims 1, 3, 5, 10, 13-14, and 16-17 were rejected under 35 U.S.C. §103(a) based on Kawan U.S. Patent Publication No. 2002/0062284 (Kawan) in view of McNair U.S. Patent No. 5,278,905 (McNair). Claim 2 was rejected under 35 U.S.C. §103(a) based on Kawan in view of McNair and further in view Chaum U.S. Patent Mo. 4,529,870 (Chaum). Claims 4, 6-9, 11-12, 15 and 18-19 were rejected under 35 U.S.C. §103(a) based on Kawan in view of McNair and further in view of Menezes et al., *Handbook of Applied Cryptography*, CRC Press, 1997 (Menezes). These grounds of rejection are addressed below following a brief discussion of the present invention to provide context.

Claims 1, 5, 7, 8, 10, 11, and 13 have been amended to be more clear and distinct. Claims 1-20 are presently pending.

The Present Invention

Personal digital assistants (PDAs) are used for storing personal information and for transferring stored personal information between computer systems. It is also possible to use a PDA to prepare and store highly confidential personal information such as transaction information for execution at a self-service terminal (SST) such as an automated teller machine (ATM).

However, to provide some security for the transaction information it would be desirable to encrypt the transaction information that is stored on and transmitted from the PDA. A conventional PDA is not an inherently secure device since it has minimal tamper resistance. In this context, minimal tamper resistance means that there is no secure area for storing a secret cryptographic key such as a separately housed encryption device adapted to the PDA. The lack of secure storage limits the use of industry-standard cryptographic techniques with a conventional PDA.

The present invention does not require a secure device for providing encryption keys. Rather, the present invention utilizes an encryption program stored in memory to generate keys for the portable terminal. A financial transaction may be initiated by the portable terminal. The encryption program determines an encryption key based on variable properties of the portable terminal. For example, a variable property would include reading contents of memory which are changed based on the usage history of the portable terminal. For example, a key may be generated from reading memory locations whose contents change when a button is selected, a pointer has moved, data has been entered, or the like. See the present application at page 2, lines 14-19, for example. The portable terminal encrypts financial information associated with the financial transaction and communicates the encrypted financial information to an ATM or other suitable self service terminal.

Section 112, Second Paragraph Rejection

Claim 7 has been amended to replace the wording "the challenge value" with the wording "the unique challenge value," to address the antecedent basis objection.

The Art Rejections

As addressed in greater detail below, Kawan, McNair, and Menezes do not support the Official Action's reading of them and the rejections based thereupon should be reconsidered and withdrawn. Further, the Applicant does not acquiesce in the analysis of Kawan, McNair, and Menezes made by the Official Action and respectfully traverses the Official Action's analysis underlying its rejections.

Claims 1, 3, 5, 10, 13-14, and 16-17 were rejected under 35 U.S.C. §103(a) based on Kawan in view of McNair. Kawan describes a contactless communication between a portable terminal and an on-line terminal of a financial transaction wherein the portable terminal receives a smart card to effect the contactless communication. As correctly admitted in the Official Action at page 4, Kawan fails to disclose means for generating a new key for a financial transaction, wherein the key is generated using one or more variable properties of the portable terminal.

McNair fails to cure the deficiencies of Kawan as a reference. McNair addresses a portable device having a microprocessor where the microprocessor develops portions of a key sequence during periods of time that the microprocessor is not engaged in performing any function necessary for the operation of the portable device. The microprocessor stores each

developed portion of the key sequence for later use in encrypting information. McNair, col. 1, line 62 – col. 2, line 2. In developing key sequence portions, McNair employs a state counter 107 and a key sequence generator 109. McNair, Fig. 1. The state counter 107 is randomly initialized and increments according to a monotonically increasing function. McNair, col. 2, lines 49-51 and col. 4, lines 34-37. The key sequence generator 109 utilizes a key variable in combination with the state counter 107 to generate key sequence portions. The contents of the state counter 107 are transmitted to a receiver in order for the receiver to generate the same key sequences. The receiver generates the same key sequences to decrypt received encrypted text by basing its key sequence generation on the received contents of the state counter. McNair, col.3, lines 12-20. The state counter 107 is implemented in software executing on the portable terminal and specifically deployed for generating portions of a key sequence. McNair, col. 2, lines 40-44.

Unlike McNair, the present invention utilizes preexisting properties of the portable terminal as a basis of generating a new key. For example, the present invention advantageously utilizes a history of usage which varies with each keystroke to create a seed for generating a unique key. Referring to page 2, lines 15-16 of the present specification, the history of usage may include button selections, pointer movements, data entered, and the like. As a result, as the usage history changes, the seed changes to produce unique keys. Furthermore, unlike McNair, the history of usage need not be transmitted. Claim 1, as presently amended, recites "means for generating a new key for the financial transaction, wherein the new key is generated using one or more variable properties of the portable terminal, the one or more variable properties include a

history of usage of the portable terminal; and means for encrypting the financial data with the new key."

See also claim 5 which recites "using one or more variable properties of the portable terminal to obtain a sequence of values for the financial transaction, the one or more variable properties include a history of usage of the portable terminal," claim 10 which recites "a portable terminal to execute an encryption program which is operable to use one or more variable properties of the portable terminal for obtaining a sequence of values, and for generating a new key based on the sequence of values, the one or more variable properties include a history of usage of the portable terminal," and claim 13 which recites "a controller executing the encryption program to generate a key for the financial transaction, wherein the key is generated using one or more variable properties of the portable terminal, the one or more variable properties include a history of usage of the portable terminal."

Despite the Official Action's admission concerning Kawan, the Official Action at page 4 relies on Kawan at para. [0031] as purportedly teaching an encrypting means when it states "it would have been obvious to a person of ordinary skill in the art to use McNair's method of key generation for the key used in Kawan's encrypting means." Applicant respectfully disagrees. Referring to para. [0031], Kawan describes authenticating a smart card. In Kawan's disclosure, the smart card contains security information. At para. [0031], Kawan states "[t]he smart card with account and/or security information is used in the opening of a transaction to identify the user's account and, through the authentication of encrypted security information, to verify that the particular card is authentic." However, unlike the present invention, Kawan is silent with

respect to how security information is encrypted. Consequently, details of how to combine a key as taught in McNair with an undisclosed encryption means as suggested by the Official Action are less than clear.

In any case, Kawan and McNair, taken separately or in combination, do not teach and do not suggest generating keys by utilizing "one or more variable properties of the portable terminal, the one or more variable properties include a history of usage of the portable terminal" as presently claimed in claim 1. The Official Action relies on McNair at col. 4, lines 28-40 as purportedly disclosing a means for generating a new key for the financial transaction, wherein the key is generated using one or more variable properties of the portable terminal. Applicant respectfully disagrees. At the cited portion of text, McNair merely describes how the initialization of the state counter 107 is based on a random number and a monotonically increasing function. Based on the monotonically increasing function, McNair's system provides an age window of acceptable random start state values such that a receiver may deem "old" random start states as invalid. Thus, McNair does not teach and does not suggest the features of the claim as suggested by the Official Action.

Furthermore, Kawan and McNair, taken seperately or in combination, do not teach and do not suggest a "means for generating a unique challenge in addition to the new key so that a unique challenge can be issued for each transaction" as presently claimed in claim 4. McNair merely provides a Data Encryption Standard (DES) algorithm which requires the same keys generated at a transmitter to be generated at a receiver. See also claims 6, 8, and 11.

Claim 2 was rejected under 35 U.S.C. §103(a) based on Kawan in view of McNair and further in view Chaum. Chaum fails to cure the deficiencies of Kawan and McNair discussed above. Since claim 2 depends from and contain all the limitations of claim 1 as presently amended, claim 2 distinguishes from the references in the same manner as claim 1.

Claims 4, 6-9, 11-12, 15 and 18-19 were rejected under 35 U.S.C. §103(a) based on Kawan in view of McNair and further in view of Menezes. Menezes is a textbook which describes from a theoretical point of view many cryptographic techniques including Symmetric-key encryption, Public-key cryptography, and Challenge-response identification. As disclosed at page 398 of Menezes, random numbers including pseudorandom numbers may be used in challenge-response mechanisms to provide uniqueness and timeliness assurances. At page 172 of Menezes, Menezes' disclosure only goes so far as to suggest that a "well-designed software random bit generator should utilize as many good sources of randomness as are available." However, Menezes disclosure does not teach and does not suggest how to generate a random number in order to generate a key as presently claimed. Thus, Menezes fails to cure the deficiencies of Kawan and McNair discussed above.

Unlike Menezes, the present invention uses one or more properties of a portable terminal to obtain a sequence of values for a financial transaction. More particularly, these one or more properties include a history of usage of the portable terminal. Claims 8 and 11, as presently amended, recite "using one or more properties of the portable terminal to obtain a sequence of values, the one or more properties include a history of usage of the portable terminal." Menezes, Kawan and McNair, taken separately or in combination, do not teach and do not suggest "using

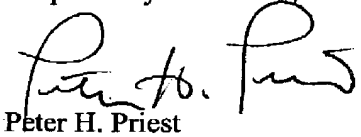
one or more properties of the portable terminal to obtain a sequence of values, the one or more properties include a history of usage of the portable terminal," as presently claimed in claims 8 and 11.

The relied upon references fail to recognize and address the problems in the manner advantageously addressed by the present claims. The claims as presently amended are not taught, are not inherent, and are not obvious in light of the art relied upon.

Conclusion

All of the presently pending claims, as amended, appearing to define over the applied references, withdrawal of the present rejection and prompt allowance are requested.

Respectfully submitted,



Peter H. Priest
Reg. No. 30,210
Priest & Goldstein, PLLC
5015 Southpark Drive, Suite 230
Durham, NC 27713-7736
(919) 806-1600